The Undecidability of FO3 and the Calculus of Relations with Just One Binary Relation

Yoshiki Nakamura

ICLA2019, March 3, 2019

Tokyo Institute of Technology, Japan

Background 1: (k-variable fragment) FO1, FO2, ..., FOk, ...

Prop. 1 (Church 1936; Turing 1937). FO (without equality) is undecidable.

Background 1: (k-variable fragment) **FO**1, **FO**2, ..., **FO**k, ...

Prop. 1 (Church 1936; Turing 1937). **FO** (without equality) is undecidable.

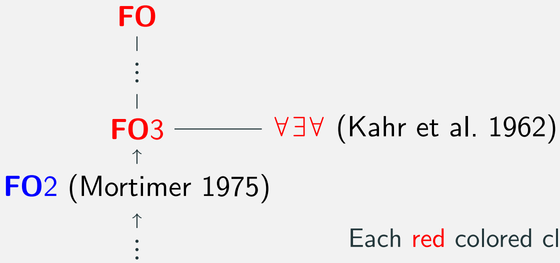
FOk: the k-variable fragment of **FO**

E.g. $\exists x.\exists y.\exists z.\exists w.a(x,y) \notin$ **FO**3 $\qquad \exists x.\exists y.\exists z.\exists x.a(x,y) \in$ **FO**3

Prop. 1 (Church 1936; Turing 1937). FO (without equality) is undecidable.

FOk: the k-variable fragment of **FO**

E.g. $\exists x.\exists y.\exists z.\exists w.a(x,y) \notin$ **FO**3 $\quad\quad$ $\exists x.\exists y.\exists z.\exists x.a(x,y) \in$ **FO**3



Each red colored class is undecidable.
Each blue colored class is decidable.

Background 2: FO over fixed signatures

FO$[(n_1, n_2, \ldots, n_k)]$: **FO** over a (relational) signature having n_1 unary relation symbols, n_2 binary relation symbols, ⋯, and having no $l(> k)$-ary relation symbols.

FO

|

⋮

|

FO$[(0, 1)]$ (Kalmár 1936)

↑

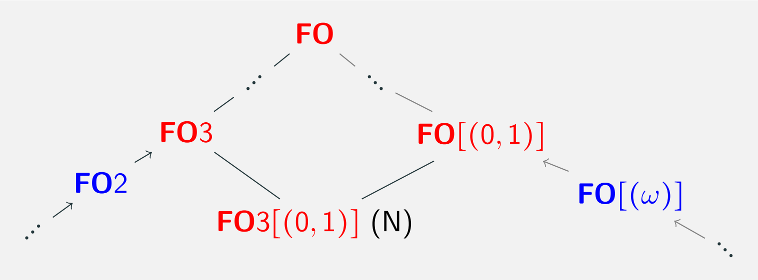
FO$[(\omega)]$ (Herbrand 1931)

↑

⋮

Contribution: FO$3[(0,1)]$ is still undecidable

Theorem 2 (N). FO$3[(0,1)]$ is undecidable.



Related Work for **FO**3

FO3

⋮

FO3$[(0,2)]$ — **FO**$^{=}$3$[(0,1)]$ (Maddux 1994)

FO3$[(\omega,1)]$ (Kahr et al. 1962; Börger et al. 1997)

⋮

FO3$[(0,1)]$ Here!

↑

FO3$[(\omega)]$ (Herbrand 1931)

↑

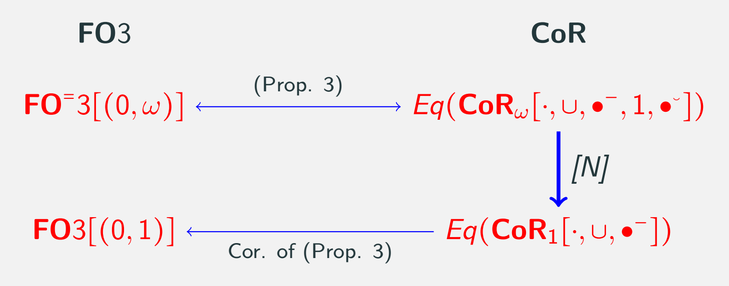
⋮

The undecidability of **FO**3$[(0,1)]$ was open.

(It was also open for the *finite validity*.)

Approach: The Calculus of Relations (CoR)

Prop. 3 (Tarski et al. 1987). There are conservative reductions[1] between the following: (1) Formulas of $\mathbf{FO}^{=}3[(0,\omega)]$; (2) Equational formulas of $\mathbf{CoR}_{\omega}$ (we denote $Eq(\mathbf{CoR}_{\omega})$).



[1] A recursive reduction preserving validity and finite validity

The Calculus of Relations (CoR)

X : a set $\qquad R, S$: binary relations on X

Operations

Identity: $1 := \{\langle x, x\rangle \mid x \in X\}$ $\qquad$ Converse: $R^{\smile} := \{\langle x, y\rangle \mid \langle y, x\rangle \in R\}$

Composition: $R \cdot S := \{\langle x, y\rangle \mid \exists z. \langle x, z\rangle \in R \wedge \langle z, y\rangle \in S\}$

Union: $R \cup S$ $\qquad$ Complement: $R^{-} := X^2 \setminus R$

Intersection: $R \cap S$ $\qquad$ Empty: $0 := \emptyset$ $\qquad$ Universality: $\top := X^2$

A: an alphabet of a size k.

Term $t, u \in \mathbf{CoR}_k ::= a \mid 1 \mid t \cdot u \mid t \cup u \mid t^{\smile} \mid t^{-}$ $(a \in A)$

Semantics: $[\![t]\!]_{\mathcal{A}} \subseteq |\mathcal{A}|^2$ (where $\mathcal{A}$ is a (first-order) model over A):

$[\![a]\!]_{\mathcal{A}}$ = "the binary relation of a on $\mathcal{A}$"; $[\![t \cdot u]\!]_{\mathcal{A}} = [\![t]\!]_{\mathcal{A}} \cdot [\![u]\!]_{\mathcal{A}}$;

$[\![t^{\smile}]\!]_{\mathcal{A}} = [\![t]\!]_{\mathcal{A}}^{\smile}$; ....

Formula $\varphi, \psi ::= t = u \mid \varphi \vee \psi \mid \neg\varphi$

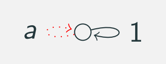
Equational Formula $\varphi, \psi \in Eq(\mathbf{CoR}_k) ::= t = u$

Toy Examples of CoR

$t \leq u$ abbreviates $t \cup u = u$.

$1 \leq a :\iff$ "(the binary relation of) a subsumes the identity relation", i.e., a is reflexive.

$a^{-} \cap 1 = 0$ also. The following can be excluded.



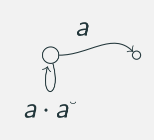
Toy Examples of CoR

$t \leq u$ abbreviates $t \cup u = u$.

$1 \leq a :\Longleftrightarrow$ "(the binary relation of) a subsumes the identity relation", i.e., a is reflexive.

$a^{-} \cap 1 = 0$ also. The following can be excluded.

$1 \leq a \cdot a^{\smile} :\Longleftrightarrow$ "every vertex has an outgoing edge of a", i.e., the domain of a is total (called left-total).



$a \cdot \top = \top$ also.

$\mathbf{FO}^=$ and CoR

(Some) $\mathbf{FO}^=$ formulas can be also expressed by (equational) formulas of **CoR**,

	$Eq(\mathbf{CoR})$	$\mathbf{FO}^=$
Reflexive	$1 \leq a$	$\forall_x . a(x,x)$
Symmetric	$a \leq a^{\smile}$	$\forall_{x,y} . a(x,y) \to a(y,x)$
Transitive	$a \cdot a \leq a$	$\forall_{x,y,z} . a(x,y) \to a(y,z) \to a(x,z)$
Dense	$a \leq a \cdot a$	$\forall_{x,y} . a(x,y) \to \exists_z . a(x,z) \wedge a(z,y)$
Functional	$a^{\smile} \cdot a \leq 1$	$\forall_{x,y,z} . a(x,y) \wedge a(x,z) \to y = z$
Left-total	$1 \leq a \cdot a^{\smile}$	$\forall_x . \exists_y a(x,y)$
$\#\lvert\mathcal{A}\rvert \geq 2$	$\top \cdot 1^- \cdot \top = \top$	$\forall_x . \exists_w . x \neq w$
$\#\lvert\mathcal{A}\rvert \geq 3$	$\top(1^- \cap (1^- 1^-))\top = \top$	$\forall_{x,y} . \exists_w . x \neq w \wedge y \neq w$
$\#\lvert\mathcal{A}\rvert \geq 4$	–	$\forall_{x,y,z} . \exists_w x \neq w \wedge y \neq w \wedge z \neq w$

$\mathbf{FO}^{=}3$ "=" CoR

Prop. 4 (Tarski et al. 1987). $\mathbf{FO}^{=}3$ and **CoR** are equivalent w.r.t. the expressive power of binary relations.

$\mathbf{FO}^{=}3 \longrightarrow$ **CoR**: (Omitted.)

CoR $\longrightarrow \mathbf{FO}^{=}3$: Let $G(t, x, y) \in \mathbf{FO}^{=}3$ be as follows:

$G(a, x, y) := a(x, y)$ for $a \in A$ $\quad G(1, x, y) := x = y$
$G(t^{-}, x, y) := \neg G(t, x, y)$ $\quad G(t \cup u, x, y) := G(t, x, y) \vee G(u, x, y)$
$G(t^{\smile}, x, y) := G(t, y, x)$ $\quad G(t \cdot u, x, y) := \exists z. G(t, x, z) \wedge G(u, z, y)$
Where x, y, and z are all distinct variables.

$\mathbf{FO}^{=}3$ "=" CoR

Prop. 4 (Tarski et al. 1987). $\mathbf{FO}^{=}3$ and **CoR** are equivalent w.r.t. the expressive power of binary relations.

$\mathbf{FO}^{=}3 \longrightarrow \mathbf{CoR}$: (Omitted.)

$\mathbf{CoR} \longrightarrow \mathbf{FO}^{=}3$: Let $G(t, x, y) \in \mathbf{FO}^{=}3$ be as follows:

$$G(a, x, y) := a(x, y) \text{ for } a \in A \quad G(1, x, y) := x = y$$
$$G(t^{-}, x, y) := \neg G(t, x, y) \quad G(t \cup u, x, y) := G(t, x, y) \vee G(u, x, y)$$
$$G(t^{\smile}, x, y) := G(t, y, x) \quad G(t \cdot u, x, y) := \exists z. G(t, x, z) \wedge G(u, z, y)$$

Where x, y, and z are all distinct variables.

Prop. 5 (Tarski et al. 1987). There are *conservative reductions* between (1) Formulas of $\mathbf{FO}3^{=}[(0, \omega)]$; (2) Formulas of $\mathbf{CoR}_{\omega}$.

((2) can be tightened to equational formulas of $\mathbf{CoR}_{\omega}$, e.g., $a = 0 \wedge b = 0$ is equivalent to $a \cup b = 0$.)

(Restated)

FO3 **CoR**

$$\mathbf{FO}^{=}3[(0,\omega)] \xrightarrow{\text{(Tarski et al. 1987)}} \mathit{Eq}(\mathbf{CoR}_{\omega}[\cdot,\cup,\bullet^{-},1,\bullet^{\smile}])$$

$$\Big\downarrow \textit{[N]}$$

$$\mathbf{FO}3[(0,1)] \xleftarrow[\text{(Tarski et al. 1987)}]{} \mathit{Eq}(\mathbf{CoR}_{1}[\cdot,\cup,\bullet^{-}])$$

We now show this, i.e., we give a conservative reduction of $\mathit{Eq}(\mathbf{CoR}_{\omega}[\cdot,\cup,\bullet^{-},1,\bullet^{\smile}]) \longrightarrow \mathit{Eq}(\mathbf{CoR}_{1}[\cdot,\cup,\bullet^{-}])$.

Outline

$$Eq(\mathbf{CoR}_\omega[\cdot, \cup, \bullet^-, 1, \bullet^\smile])$$

$\downarrow$ 1. converse elim.

$$Eq(\mathbf{CoR}_\omega[\cdot, \cup, \bullet^-, 1])$$

$\downarrow$ 3. reducing characters (using 1)

$$Eq(\mathbf{CoR}_1[\cdot, \cup, \bullet^-, 1])$$

$\downarrow$ 2. identity elim.

$$Eq(\mathbf{CoR}_2[\cdot, \cup, \bullet^-])$$

$\downarrow$ 4. reducing characters (not using 1)

$$Eq(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$$

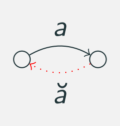
$\breve{A}$: a set of characters disjoint with A.

$\breve{a} \in \breve{A}$: a character for the converse of $a \in A$. (Note: $\breve{a} \not\equiv a^{\smile}$)

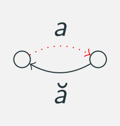
Lemma 6 (N). $\breve{a}$ expresses the converse of a on any model satisfying the following equations:

(Ca.1) $(a \cdot \breve{a}^{-}) \cap 1 = 0$ (Ca.2) $(\breve{a} \cdot a^{-}) \cap 1 = 0$

Proof. Because the following cases can be excluded.



Then (Ca.1) fails.



Then (Ca.2) fails.

(Each red colored edge denotes that the edge does not exist.)

1.2. Elimination of Converse ($\bullet^{\smile}$)

$\breve{a}$: a character expressing the converse of a.

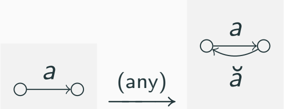
$CF(t)$: the normal form of t in the following rewriting rules:

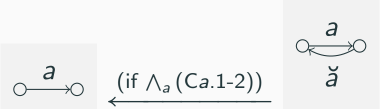
$$a^{\smile} \rightsquigarrow \breve{a} \qquad 1^{\smile} \rightsquigarrow 1 \qquad (t \cdot u)^{\smile} \rightsquigarrow u^{\smile} \cdot t^{\smile}$$

$$(t \cup u)^{\smile} \rightsquigarrow t^{\smile} \cup u^{\smile} \qquad (t^{-})^{\smile} \rightsquigarrow (t^{\smile})^{-} \qquad (t^{\smile})^{\smile} \rightsquigarrow t.$$

Theorem 7 (N). $t = u$ is valid iff $\bigwedge_a (\mathrm{C}a.1\text{-}2) \to CF(t) = CF(u)$ is.

Proof.
If there is a counter model of $t = u$, then there is a counter model of $\bigwedge_a (\mathrm{C}a.1\text{-}2) \to CF(t) = CF(u)$, and vice versa.





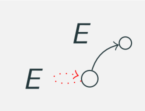
□

$\rightsquigarrow$ Converse can be replaced by characters!

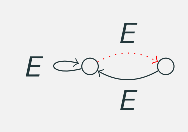
E: a character for the identity.

Lemma 8 (N). E expresses an equivalence relation if the following holds: (E1) $(E \cdot \top) = \top$ (E2) $(E^{-} \cdot E) \cap E = 0$ (E3) $(E \cdot E^{-}) \cap E = 0$ (E4) $(E \cdot E) \cap E^{-} = 0$ (Actually (E3) and (E4) are redundant.)

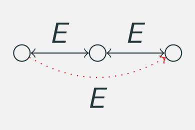
Proof. Because the following cases can be excluded.



If not reflexive, (E2) fails by (E1).



If not symmetric, (E2) fails by the reflexivity.

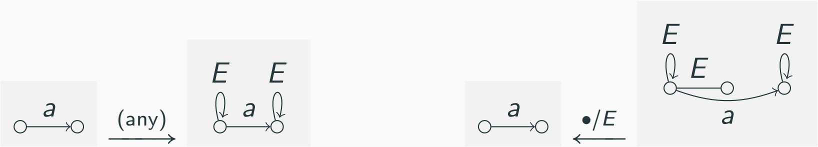


If not transitive, (E2) fails by the symmetric.

E: a character denoting an equivalence relation.
$IF(t)$: the term t without 1 defined by $IF(a) := EaE$; $IF(1) := E$; $\cdots$.
E.g. $IF(ab \cap 1) := (EaE)(EbE) \cap E$.

Theorem 9 (N). $t = u$ is valid iff (E1-4) $\to IF(t) = IF(u)$ is valid.

Proof. A counter model of $t = u$ induces a counter model of (E1-4) $\to IF(t) = IF(u)$, and vice versa.



⇝ The identity relation can be replaced by a character!

Outline

$$Eq(\mathbf{CoR}_\omega[\cdot, \cup, \bullet^-, 1, \bullet^\smile])$$

↓ 1. converse elim.

$$Eq(\mathbf{CoR}_\omega[\cdot, \cup, \bullet^-, 1])$$

↓ 3. reducing characters (using 1)

$$Eq(\mathbf{CoR}_1[\cdot, \cup, \bullet^-, 1])$$

↓ 2. identity elim.

$$Eq(\mathbf{CoR}_2[\cdot, \cup, \bullet^-])$$

↓ 4. reducing characters (not using 1)

$$Eq(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$$

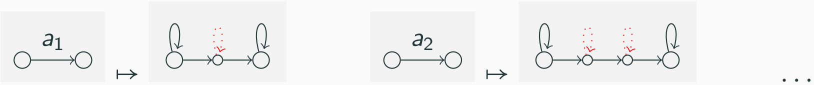
3. Reducing Characters (Using 1)

Let A be the set $\{a_1, \ldots, a_n\}$.

$\mathrm{T}_1(t)$: the term with only the character a defined by

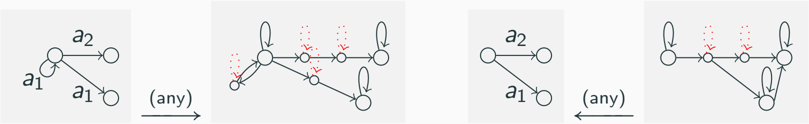
$\mathrm{T}_1(a_i) \coloneqq (a \cap 1)a((a^{-} \cap 1)a)^{i}(a \cap 1)$; $\mathrm{T}_1(1) \coloneqq (a \cap 1)$;

$\mathrm{T}_1(t^{-}) \coloneqq (a \cap 1)\mathrm{T}_1(t)^{-}(a \cap 1)$; $\cdots$.

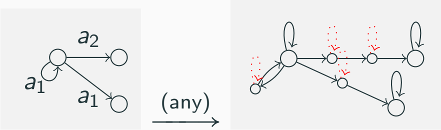


Theorem 10 (N). $t = u$ is valid iff $\mathrm{T}_1(t) = \mathrm{T}_1(u)$ is valid.

Proof.



Observation of 3. (Reducing Characters Using 1)



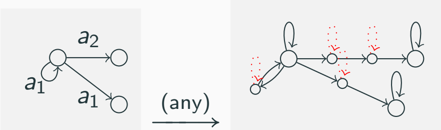
Roughly speaking, the following two are the keys:

(1) the universal relation of the pre-translated model is definable.

$\ddot{t} := (a \cap 1)$ denotes the universal relation in the above.

(2) $\mathrm{T}_1(a_i)$ preserves the relation of a_i on the pre-translated model.

Observation of 3. (Reducing Characters Using 1)



Roughly speaking, the following two are the keys:

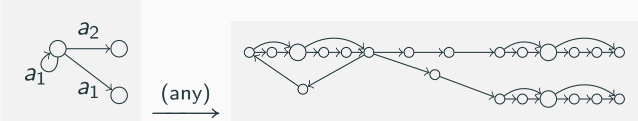
(1) the universal relation of the pre-translated model is definable.

$\ddot{t} := (a \cap 1)$ denotes the universal relation in the above.

(2) $\mathrm{T}_1(a_i)$ preserves the relation of a_i on the pre-translated model.

How to construct this-like reduction without 1 (nor converse)?

4. $Eq(\mathbf{CoR}_2[\cdot, \cup, \bullet^-]) \longrightarrow Eq(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$



(1): $\ddot{t} := ((a \cap a^3)\top) \cap (\top(a \cap a^2))$ expresses the universal relation.

(2): $\mathsf{T}_2(a_i) := (a \cap a^3)a^{i+1}(a \cap a^2)$ preserves a_i.

(In general ($cod(\ddot{t}) \neq dom(\ddot{t})$), there may be no decoder in the above. So, we should exclude these cases.)

Lemma 11 (N). $cod(\ddot{t}) = dom(\ddot{t})$ holds iff
(Ax.1) $(a \cap a^3)\top = (a \cap a^2)(a \cap a^3)\top$;
(Ax.2) $\top(a \cap a^2) = \top(a \cap a^2)(a \cap a^3)$.

Theorem 12 (N). $t = u$ is valid iff (Ax.1-2) $\rightarrow \mathsf{T}_2(t) = \mathsf{T}_2(u)$ is.

Conclusion

We gave conservative reductions for reducing operations (of CoR) or the number of characters.

Theorem. The validity and finite validity are undecidable for

1. $\mathbf{FO}3[(0,1)]$; and
2. $\mathit{Eq}(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$.

Open Problem

Is $\mathit{Eq}(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$ a minimal undecidable class?

$\mathit{Eq}(\mathbf{CoR}_1[\cdot, \cup, \bullet^-])$ (N)

- $\mathit{Eq}(\mathbf{CoR}_1[\cdot, \cup])$ (Andréka et al. 1995)
- $\mathit{Eq}(\mathbf{CoR}_1[\cdot, \bullet^-])$ ((un)decidable?)
- $\mathit{Eq}(\mathbf{CoR}_1[\cup, \bullet^-])$ (Andréka et al. 1995)

Thank you!

References

Andréka, Hajnal and D. A. Bredikhin (Dec. 1995). "The equational theory of union-free algebras of relations". In: *Algebra Universalis* 33.4, pp. 516–532. ISSN: 00025240. DOI: 10.1007/BF01225472.

Börger, Egon, Erich Grädel, and Yuri Gurevich (1997). *The Classical Decision Problem*. Springer, p. 482. ISBN: 3540423249.

Church, Alonzo (June 1936). "A note on the Entscheidungsproblem". In: *The Journal of Symbolic Logic* 1.01, pp. 40–41. ISSN: 0022-4812. DOI: 10.2307/2269326.

Herbrand, Jacques (1931). "Sur le problème fondamental de la logique mathématique". In: *Sprawozdania z posiedezen Towarzysta Naukowego Warszawskiego, Wydzial III* 24, pp. 12–56.

Kahr, A. S., Edward F. Moore, and Hao Wang (Mar. 1962). "Entscheidungsproblem reduced to the AEA case". In: *Proceedings of the National Academy of Sciences* 48.3, pp. 365–377. ISSN: 0027-8424. DOI: 10.1073/pnas.48.3.365.

Kalmár, László (1936). “Zuriickftihrung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen, bindren, Funktionsvariablen”. In: *Compositio mathematica* 4.

Maddux, Roger D. (June 1994). “Undecidable semiassociative relation algebras”. In: *The Journal of Symbolic Logic* 59.02, pp. 398–418. ISSN: 0022-4812. DOI: 10.2307/2275397.

Mortimer, Michael (Jan. 1975). “On languages with two variables”. In: *Mathematical Logic Quarterly* 21.1, pp. 135–140. ISSN: 09425616. DOI: 10.1002/malq.19750210118.

Tarski, Alfred and Steven Givant (1987). *A formalization of set theory without variables*. Vol. 41. Colloquium Publications. American Mathematical Society, p. 318. ISBN: 0821810413.

Turing, A. M. (Jan. 1937). “On Computable Numbers, with an Application to the Entscheidungsproblem”. In: *Proceedings of* *the London Mathematical Society* s2-42.1, pp. 230–265. ISSN: 00246115. DOI: 10.1112/plms/s2-42.1.230.